EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Tina Gonka on 2 December 2009.

3. The application has been amended as follows:

Claim 24 (Currently amended) A method for transmitting data, comprising:

providing each of a plurality of users of a public communication network with a secret encryption program and a secret algorithm for generating an encryption key;

by a first user of the public communication network:

receiving a first random value originating from useful data produced in a first stochastic process;

generating a first symmetrical encryption key based on the first random value using the secret algorithm;

transmitting the first random value to a second user remote from the first user over the public communication network;

by the second user:

receiving the first random value from the first user; and

generating the first symmetrical encryption key based on the received random value using the secret algorithm;

the first and second users then encrypting and communicating the useful data over the public communication network using the secret encryption program and the first symmetrical encryption key; and

wherein the first random value comprises a digital value derived from the useful data;

wherein the first user comprises a remote maintenance device;

the second and remaining users comprise respective automation devices connected to each other by a bus;

each of the respective automation devices obtaining plural random values of stochastic data;

combining two different subsets of the plural random values, producing two different data words;

communicating the two different data words to the respective automation devices and to the remote maintenance device;

inputting the two different data words into two different encryption programs that are identical in each of the respective automation devices and the remote maintenance device;

generating two different symmetrical encryption keys from the two different data words via the two different encryption programs in each of the respective automation devices and the remote maintenance device; and

communicating encrypted data using one or the other of the two different symmetrical encryption keys at a given time among the respective automation devices and the remote maintenance device; and

switching between the two different symmetrical encryption keys at a predetermined time among all of the respective automation devices and the remote maintenance device at once.

Claim 40 (Currently amended) A communication system, comprising:

at least first and second users remote from each other; and

a public communication network for transmitting data between the at least first and second users,

the first user comprising:

a first receiver for receiving a first random value originating from useful data produced by a stochastic process,

an encryption key generator for generating a first symmetrical encryption key based on the first random value,

a storage unit for storing the first symmetrical encryption key, and

a transmitter for transmitting the first random value to the second user via the public communication network;

the second user comprising:

a first receiver for receiving the first random value from the first user, and

an encryption key generator for generating the first symmetrical encryption key based on the first random value received from the first user,

wherein data transferred between the users is encrypted and unencrypted via the first symmetrical encryption key; and

wherein the first random value comprises a first digital value derived from a first useful datum;

wherein the first user comprises a remote maintenance device;

the second and remaining users comprise respective automation devices connected to each other by a bus;

each of the respective automation devices obtaining plural random values of stochastic data;

combining two different subsets of the plural random values, producing two different data words;

communicating the two different data words to the respective automation devices and to the remote maintenance device;

inputting the two different data words into two different encryption programs that are identical in each of the respective automation devices and the remote maintenance device;

generating two different symmetrical encryption keys from the two different data words via the two different encryption programs in each of the respective automation devices and the remote maintenance device; and

communicating encrypted data using one or the other of the two different symmetrical encryption keys at a given time among the respective automation devices and the remote maintenance device; and

switching between the two different symmetrical encryption keys at a predetermined time among all of the respective automation devices and the remote maintenance device at once.

Claim 47 (Currently amended) A method for transmitting data, comprising:

by a first user of a public communication network:

storing a first random measured value received from a first stochastic process;

generating a first symmetrical encryption key based on the first random measured value;

transmitting the first measured random value to a second user remote from the first user on the public communication network;

receiving a second random measured value from the second user;

generating a second symmetrical encryption key based on the received random value;

by the second user:

storing the second random measured value received from a second stochastic process;

generating the second symmetrical encryption key based on the second random measured value;

transmitting the second random measured value to the first user;

receiving the first random measured value from the first user;

generating the first symmetrical encryption key based on the received first random measured value,

wherein the first symmetrical encryption key is used to encrypt data transmitted between the first and second users during a first time interval, and the second symmetrical encryption key is used to encrypt data transmitted between the first and second users during a second time interval; and

wherein the first and second random measured values each comprise a respective useful datum from a respective different sensor indicating an operational measurement of an automation system;

wherein the first user comprises a remote maintenance device;

the second and remaining users comprise respective automation devices connected to each other by a bus;

each of the respective automation devices obtaining plural random values of stochastic data;

combining two different subsets of the plural random values, producing two different data words;

communicating the two different data words to the respective automation devices and to the remote maintenance device;

inputting the two different data words into two different encryption programs that are identical in each of the respective automation devices and the remote maintenance device;

generating two different symmetrical encryption keys from the two different data words via the two different encryption programs in each of the respective automation devices and the remote maintenance device; and

communicating encrypted data using one or the other of the two different symmetrical encryption keys at a given time among the respective automation devices and the remote maintenance device; and

switching between the two different symmetrical encryption keys at a predetermined time among all of the respective automation devices and the remote maintenance device at once.

Claim 53 (Cancelled)

DETAILED ACTION

4. The amendment of 19 August 2009 has been noted and made of record.

5. Claims 24, 28, 30, 33-35, 37, 40-43, and 45-52 are pending.

6. Claims 1-23, 25-27, 29, 31, 32, 36, 38, 39 and 44 have been cancelled as per applicant's amendment.

7. Claim 53 has been cancelled by the examiner's amendment above.

Allowable Subject Matter

8. Claims 24, 28, 30, 33-35, 37, 40-43, and 45-52 are allowed.

9. The following is an examiner's statement of reasons for allowance:

The examiner's amendment above has put the case in condition for allowance. The addition of claim 53 defines the operating environment in such a way as to distinguish the instant application from the prior art.

10. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

12. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

13. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf